Zumigo
Mobile in Context

Zumigo/FCC Meeting

December 5, 2017

Agenda

- Why are we here?
- Trends
- The Problem
- Major Issues
- Solutions
- Conclusion

Why are we here?

Zumigo
Mobile in Context

2016 & 2017 marked the largest data breaches in US history:

Equifax (2017): 143,000,000

Uber (2016): 57,000,0000

Yahoo (2016): 3,000,000,000

MySpace (2016): 360,000,000

Home Depot (2014): 56,000,000

Target (2012): 40,000,000

Why are we here?

- In the aftermath of these breaches, Zumigo provides solutions that leverage the fact that every consumer has a mobile phone.
- Due to several factors, these solutions are still largely underutilized in the marketplace.

We need the FCC's help to make mobile real-time account information more readily usable so that consumers can be protected from identity theft and account takeover.

Trends

- We have entered a new era where every consumer has a mobile phone and they are transacting more and more on them.
- Mobile carriers have valuable information that can help protect consumers from identity theft and fraud, because it helps to identify WHO a person is and WHERE they are. It can also help to prevent mobile hijacking.
- However, in their pursuit to protect consumer privacy by requiring burdensome/complex consent language to access mobile information, carriers are actually leaving consumers at risk, when they could actually be protecting them more.

Trends

Zumigo
Mobile in Context

Mobile Hijacking - Fraudsters hijack mobile phones by:

- Impersonating the consumer to do a "SIM swap" (i.e. asking the carrier to move the consumer's number to a different device and SIM card), so that all calls and texts are sent to the fraudster's device.
- Breaking into a consumer's online mobile account and enabling call forwarding to so that all incoming calls go directly to the fraudster.
- Porting a consumer's mobile number to another carrier so that calls and texts go to the fraudster's device.

Once a mobile phone is hijacked, it becomes very easy to break into the consumer's online accounts by intercepting calls and one-time passcodes.

The Problem

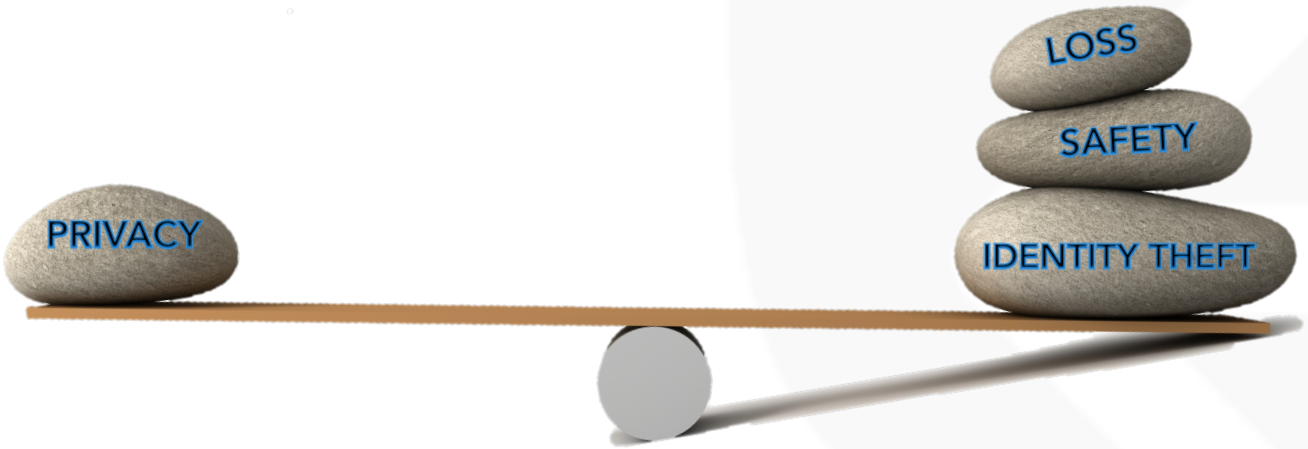
- Regulatory policies have not kept up with the pace at which mobile phones are becoming an integral part of people's lives. Consumers are using mobile phones for:
  - Online banking
  - Securing their homes
  - Accessing hotel rooms
  - Driving their cars
- Privacy has been the main focus, but the safety and security of the consumer must also be considered.

We strongly believe that if consumers understood the vulnerabilities they face, and their carrier's ability to help prevent it, they would want the carrier data to be shared in order to keep them safe.

The Problem

Zumigo
Mobile in Context

As breaches become more prevalent and as consumers rely more on mobile phones, there is a tipping point where financial and personal protections begin to equal, or outweigh, privacy concerns.



Major Issues - Fear

- Because FCC guidelines around the use of carrier data have been fairly broad and privacy-focused, carriers are independently coming up with their own interpretations of what is - and is not - allowed.
- Risk-averse carriers are very concerned about fines and lawsuits. This has resulted in:
  - Policies that are far more restrictive than the FCC guidelines.
  - Long and ineffective legal and privacy review processes, which are not scalable.
- All of this fear, uncertainty, and indecisiveness has caused a huge log jam that is stifling necessary progress.

It took 8 months to get one of the nation's largest banks approved to simply verify that the mobile number, name, and address on a new account application matches what is on file at the carrier.

Major Issues – Consent

- The consent requirements are far more burdensome for carrier data compared to other kinds of data that are much more sensitive.

EXAMPLE: Standard consent language for pulling all types of FCRA and GLBA-regulated data (broad language encompasses all data sources):

By selecting Continue**, you authorize us to obtain a credit report or other report or account information from credit or information services agencies** to help verify the information you provide in this application; for consideration of other accounts and services, and for any other lawful purpose. If your information does not meet certain qualifications, you will not be able to proceed with your application at this time.

SAMPLE: Carrier language requirements (specific language that constantly changes):

You authorize your wireless operator to disclose information about your account, subscriber status, billing and payment method, device details, call forwarding status (including the number to which your device is forwarded), and device location information, if available, to support identity verification, fraud avoidance and other uses in support of transactions for the duration of your business relationship with us. This information may also be shared by us with other companies to support your transactions with us and for identity verification and fraud avoidance purposes. This information includes Customer Proprietary Network Information (CPNI), which is information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service. It is your right and your carrier's duty under federal law to protect your CPNI. Your decision will not affect your current wireless service.

The carrier language is arduous, confusing to consumers, and longer than the language for all other data sources combined. It also alerts fraudsters to exactly how fraud is being detected, allowing them to adapt.

Major Issues - Inconsistencies

- The four major carriers have different interpretations of FCC guidelines related to the release of carrier data which results in:
  - Inconsistencies in, and constantly changing, consent language requirements
    - Example: one carrier has already changed the consent language requirements twice in the past year.
  - Inconsistencies in, and constantly changing, usage rules and requirements
    - No consent vs. implicit consent vs. explicit consent vs. SMS confirmation
      - Example: some carriers allow some data elements to be released without consent for fraud prevention, while other do not.
    - TCPA usage
      - Example: Three major carriers allow the use of carrier data to prevent TCPA violations, while one does not.
    - CPNI versus non-CPNI data
      - Example: One major carriers believes that a call forwarding indicator is CPNI, while the other three do not.
    - Storage restrictions
      - Example: Carriers do not allow storage of most data elements, but there are valid reasons why the data may need to be stored.

Solutions - Guidance

- Provide specific, but promotive, guidelines around the use of mobile carrier data – especially when it is used to protect consumers from fraud:
  - What can be shared
  - How it can be shared
  - Consent requirements
  - Usage guidelines
  - Storage guidelines

- Provide guidelines that are consistent across data types
  - Currently, the requirements are totally different for mobile location information versus mobile identity information (i.e. subscriber, account, and device information) - **even when the data is used solely for fraud prevention.**

Solutions - Guidance

Zumigo
Mobile in Context

- FCRA and GLBA are great examples of regulations that have made data accessible in a safe, but scalable way.
- Although credit data is extremely sensitive in nature, it is necessary to make it accessible for the good of society and our nation's economy.
  - Billions of FCRA and GLBA-regulated reports are released each year. As a result:
    - Lenders make better decisions and comply with regulations
    - Consumers can get the credit they need.
    - Consumers are better protected against identity theft and account takeover.
- Having more clearly defined rules and regulations for releasing mobile carrier data would help to alleviate fears of lawsuits while protecting carriers, businesses, and **consumers**.

Solutions - Consent

- Remove the consent requirement of stating that information is being released by the "carrier".
- Instead, allow more flexible language, such as:
  - *"You authorize the bank and its service providers to use your mobile account for verifying your identity and protecting you from fraud."*

****

- Make the release of carrier data opt-out, rather than opt-in, when it is being used to prevent fraud and identity theft.

****

- Create a national registry for consumers to opt-in to allow their mobile information to be used for fraud prevention purposes.

Solutions - Consent

Benefits of a National Registry:

- The National Registry would be a central database where consumers could opt-in and opt-out for use of their mobile account information to prevent identity theft and fraud.
- Consumers would feel safe and protected with full transparency.
- Businesses such as carriers, banks, and merchants can rely on the registry to identify consumers that have opted in or out. This would help to:
  - Relieve the burden of legal and privacy issues on the carriers.
  - Relieve the burden of collecting consent and updating Terms & Conditions for banks, merchants, and others that need access to the mobile information.

Conclusion

Zumigo
Mobile in Context

"Regulatory gaps exist because laws have not kept up with advances in technology. The gaps are getting wider as technology advances ever more rapidly."

- Vivek Wadhwa

Fellow at Arthur & Toni Rembe Rock Center for Corporate Governance, Stanford University

Zumigo
Mobile in Context

Thank You

Chirag Bakshi
chirag@zumigo.com

Lyndi Long
lyndi@zumigo.com

Jong Lee
jong@zumigo.com